REVISTA DE LA
UNIÓN MATEMÁTICA ARGENTINA
Vol. 53, No. 1, 2012, 1–9

CONJUNTOS SUMA PEQUEÑOS EN GRUPOS HAMILTONIANOS

WILSON F. MUTIS, FERNANDO A. BENAVIDES, AND JOHN H. CASTILLO

Abstract. Given a group $(G,\cdot)$ and positive integers $r,s \leq |G|$, we denote with $\mu_G(r,s)$ the least possible size of the sumsets $AB = \{a\cdot b : a \in A \text{ and } b \in B\}$, where A, B run over all subsets of G, such that $|A| = r$ and $|B| = s$. Let $H = \mathcal{Q} \times (\mathbb{Z}/2\mathbb{Z})^k \times \mathcal{C}$ be a Hamiltonian group, where k is a non-negative integer, $\mathcal{Q}$ is the quaternion group of 8 elements and $\mathcal{C}$ is a cyclic group of odd order. We present an explicit formula for $\mu_H(r,s)$.

Resumen. Dados un grupo $(G,\cdot)$ y enteros positivos $r,s \leq |G|$, se denota con $\mu_G(r,s)$ el menor cardinal posible de los conjuntos suma $AB = \{a\cdot b : a \in A \text{ and } b \in B\}$, donde A, B recorren los subconjuntos de G, tales que $|A| = r$ y $|B| = s$. Sea $H = \mathcal{Q} \times (\mathbb{Z}/2\mathbb{Z})^k \times \mathcal{C}$ un grupo hamiltoniano, donde k es un entero no negativo, $\mathcal{Q}$ es el grupo cuaternión de 8 elementos y $\mathcal{C}$ es cíclico de orden impar. Se presenta una fórmula explícita para la función $\mu_H(r,s)$.

1. Introducción

Sea $(G,\cdot)$ un grupo. El conjunto suma (o conjunto producto) de dos subconjuntos A y B de G es el conjunto denotado con AB y definido por

$$AB = \{a\cdot b \ : \ a \in A \text{ y } b \in B\}.$$

Además si $A = \varnothing$ o $B = \varnothing$, se define $AB = \varnothing$. Dados dos enteros r, s tales que $1 \leq r, s \leq |G|$, $\mu_G(r,s)$ denota al mínimo cardinal de los conjuntos producto AB, donde A y B son subconjuntos de G de cardinal r, s, respectivamente, es decir,

$$\mu_G(r,s) = \text{mín}\{\ |AB| \ : \ A, B \subset G,\ |A| = r, |B| = s\ \}.$$

Determinar una fórmula explícita que facilite el cálculo de $\mu_G(r,s)$ es un problema de interés en la Teoría Aditiva de Números. El primer resultado en esta dirección, según [5], es el Teorema de Cauchy-Davenport. Este teorema establece que, para un grupo cíclico G de orden primo p, $\mu_G(r,s) = \text{mín}\{p, r+s-1\}$.

Para el caso en que G es un grupo abeliano, Eliahou y Kervaire probaron en [2] que

$$\mu_G(r,s) = \kappa_G(r,s) \tag{1}$$

donde

2000 *Mathematics Subject Classification.* 11B13.
Key words and phrases. Conjunto Suma, Grupo cuaternión, Grupo hamiltoniano.

$$\kappa_G(r,s) = \min_{h\in\mathcal{H}(G)} \left\{ \left(\left\lceil \frac{r}{h} \right\rceil + \left\lceil \frac{s}{h} \right\rceil - 1 \right) h \right\}$$

y $\mathcal{H}(G)$ es el conjunto de órdenes de subgrupos finitos de G. Por ejemplo, si G es abeliano de orden finito n, $\mathcal{H}(G)$ coincide con el conjunto de divisores positivos de n y en este caso

$$\mu_G(r,s) = \min_{d|n} \left\{ \left(\left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1 \right) d \right\}.$$

Cuando G es un grupo finito no abeliano se desconoce una fórmula explícita de $\mu_G(r,s)$, aunque existen grupos no abelianos para los cuales la igualdad (1) se cumple. Por ejemplo en [10] Kemperman demostró que $\mu_G(r,s) = \kappa_G(r,s)$ cuando G es un grupo libre de torsión, Eliahou y Kervaire en [3] probaron que esta igualdad también se satisface para grupos diédricos de orden $2p^n$ con p primo y posteriormente en [7] ellos extendieron la fórmula a la clase de grupos diédricos finitos. Sin embargo, la igualdad (1) no se verifica para todo grupo finito no abeliano, ya que el producto semidirecto $G = C_{13} \ltimes C_3$, donde C_i denota el grupo cíclico de orden i, cumple la desigualdad $\mu_G(6,6) > \kappa_G(6,6)$ (ver [6]).

El objetivo de este artículo es ampliar la clase de grupos finitos no abelianos que cumplen la identidad (1). Sea $\mathcal{Q}$ el grupo cuaternión de 8 elementos y k un entero no negativo. En la siguiente sección se prueba que $\mu_{\widehat{H}}(r,s) = \kappa_{\widehat{H}}(r,s)$ para el grupo $\widehat{H} = \mathcal{Q} \times (\mathbb{Z}/2\mathbb{Z})^k$ y, a partir de este hecho, se muestra que $\mu_H(r,s) = \kappa_H(r,s)$ para el grupo hamiltoniano $H = \mathcal{Q} \times (\mathbb{Z}/2\mathbb{Z})^k \times \mathcal{C}$ donde $\mathcal{C}$ es un grupo cíclico de orden impar.

En lo que sigue serán necesarias las siguientes definiciones y resultados.

Definición 1.1. *Se dice que un grupo no abeliano G es hamiltoniano si todos sus subgrupos son normales.*

Se puede probar que el grupo cuaternión $\mathcal{Q}$ es un grupo hamiltoniano y, más aún, que todo grupo hamiltoniano H es de la forma $H = \mathcal{Q} \times (\mathbb{Z}/2\mathbb{Z})^k \times G$, donde G es un grupo abeliano en el cual todos sus elementos son de orden finito impar (ver Teorema 5.3.7 de [11]).

En el Lema 2.1 y los Teoremas 4.1, 4.2 y 4.6 de [5], se establecen las siguientes propiedades.

Lema 1.1. *Sean G un grupo finito y r, s enteros tales que $1 \le r, s \le |G|$. Entonces*

1. $\mu_G(r,s) = \mu_G(s,r)$.
2. *Si $1 \le r \le 3$, entonces $\mu_G(r,s) = \kappa_G(r,s)$.*
3. *Si $r + s > |G|$, entonces $\mu_G(r,s) = \kappa_G(r,s) = |G|$.*
4. *Si $r + s = |G|$, entonces $\mu_G(r,s) = \kappa_G(r,s)$.*

En el Lema 2.2 de [3], se prueba la siguiente desigualdad.

Lema 1.2. *Sea G un grupo soluble finito y r, s enteros tales que $1 \le r, s \le |G|$. Si k es el orden de un subgrupo normal K de G, entonces*

$$\mu_G(r,s) \le \left(\left\lceil \frac{r}{k} \right\rceil + \left\lceil \frac{s}{k} \right\rceil - 1 \right) k.$$

Definición 1.2. *Se dice que un grupo G es supersoluble si admite una serie normal $G = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_k = \{1\}$, donde para cada $i = 1, 2, \ldots, k$ el grupo factor N_{i-1}/N_i es cíclico.*

Los grupo finitos supersolubles satisfacen la siguiente propiedad, ver Corolario 10.5.2 en [9].

Teorema 1.1. *Sean $p_1 \leq p_2 \leq \cdots \leq p_r$ números primos. Si G es un grupo finito supersoluble de orden $p_1 p_2 \cdots p_r$, entonces G tiene una serie principal*

$$G = N_0 \supset N_1 \supset \cdots \supset N_r = \{1\},$$

donde para cada $i = 1, 2, \ldots, r$ el grupo factor N_{i-1}/N_i es de orden p_i.

Corolario 1.1. *Sea p un número primo. Si G es un p-grupo finito, entonces para cada divisor positivo t de $|G|$ existe un subgrupo normal N de G tal que $|N| = t$.*

Demostración. Por los Teoremas 10.2.4 y 10.3.4 de [9] sabemos que G es un grupo supersoluble. Además, como $|G| = p^n$, del Teorema 1.1 se deduce que G tiene una serie principal

$$G = H_0 \supset H_1 \supset \cdots \supset H_n = \{1\},$$

donde $|H_{i-1}| = p|H_i|$ para cada i. Dado que $|H_n| = 1$, entonces $|H_{i-1}| = p^{n-i+1}$ para cada $i \in \{1, \ldots, n\}$.

Sea t un divisor positivo de $|G|$, luego $t = p^k$ con $0 \leq k \leq n$. Si $k = 0$ entonces $H_n = \{1\}$ es un subgrupo normal de G y $|H_n| = 1$. Si $k = n$, $N = G$ satisface el enunciado del corolario. Por último, si $k = 1, \ldots, n-1$ entonces H_{n-k} es un subgrupo normal de G y $|H_{n-k}| = k$. □

Definición 1.3. *Sean $\mathcal{V}$ un conjunto ordenado con elemento mínimo a_0 y t un entero positivo. El subconjunto $I_t = \{a_0 < a_1 < \cdots < a_{t-1}\}$ de $\mathcal{V}$ se denomina el conjunto inicial de longitud t si para todo $i \in \{0, 1, \ldots, t-2\}$ se tiene $\{x \in \mathcal{V} : a_i < x < a_{i+1}\} = \varnothing$. El conjunto $I_0 = \varnothing$ es el segmento inicial de longitud cero.*

2. La función μ_H para grupos hamiltonianos.

Sea $H = \mathcal{Q} \times (\mathbb{Z}/2\mathbb{Z})^k \times \mathcal{C}$, donde k es un entero no negativo, $\mathcal{Q}$ es el grupo cuaternión de 8 elementos y $\mathcal{C} = \langle g \rangle$ es un grupo cíclico de orden impar.

Lema 2.1. *El grupo H es soluble.*

Demostración. Observemos que $\widehat{H} = \mathcal{Q} \times (\mathbb{Z}/2\mathbb{Z})^k$ es un subgrupo normal de H de índice impar, entonces por el Teorema de Feit-Thompson, ver [8], $H/\widehat{H}$ es soluble. Además $\widehat{H}$ es soluble por ser un 2-grupo y, por lo tanto, H es soluble. □

Lema 2.2. *Si $|\mathcal{C}| = n$ entonces el conjunto $\mathcal{H}(H)$ de órdenes de subgrupos de H es*

$$\mathcal{H}(H) = \{\ 2^x d\ :\ 0 \leq x \leq k+3,\ d|n\ \}.$$

Demostración. Sea $x \in \{0, 1, \ldots, k+3\}$ y d un divisor positivo de n. Entonces por el Corolario 1.1 existe un subgrupo normal $\mathcal{T}$ de $\widehat{H}$ tal que $|\mathcal{T}| = 2^x$. Como $\mathcal{C}$ es cíclico de orden n existe un subgrupo normal N de $\mathcal{C}$ de orden d, luego $\mathcal{T} \times N$ es un subgrupo normal de H de orden $2^x d$.

Ahora si m es el orden de un subgrupo de H entonces m divide a $|H| = 2^{k+3}n$, y dado que 2 no divide a n, se tiene que $m = 2^x d$ para algún $x \in \{0, 1, \ldots, k+3\}$ y algún divisor positivo d de n. □

El siguiente lema es una consecuencia directa del Lema 1.1.

Lema 2.3. *Sea $\mathcal{Q}$ el grupo de los cuaterniones. Si r y s son dos enteros positivos menores o iguales a 8, entonces $\mu_{\mathcal{Q}}(r, s) = \kappa_{\mathcal{Q}}(r, s)$.*

Lema 2.4. *Sean $k \geq 1$, $\widehat{H} = \mathcal{Q} \times (\mathbb{Z}/2\mathbb{Z})^k$ y $T = \mathcal{Q} \times (\mathbb{Z}/2\mathbb{Z})^{k-1}$. Entonces para toda terna de enteros positivos $r, s_0, s_1 \leq |T|$ se cumple la desigualdad*

$$\kappa_T(r, s_0) + \kappa_T(r, s_1) \geq \kappa_{\widehat{H}}(r, s_0 + s_1).$$

Demostración. Dado que todo p-grupo finito es supersoluble, por el Corolario 1.1 se tiene que el conjunto de órdenes de subgrupos de T es el conjunto de divisores de $|T|$; es decir $\mathcal{H}(T) = \{1, 2, 2^2, \ldots, 2^{k+2}\}$.

Sean r, s_0, s_1 enteros positivos tales que $r, s_0, s_1 \leq |T|$ y $x, y \in \{0, 1, \ldots, k+2\}$ tales que

$$\kappa_T(r, s_0) = 2^x \left(\left\lceil \frac{r}{2^x} \right\rceil + \left\lceil \frac{s_0}{2^x} \right\rceil - 1 \right) \quad \text{y} \quad \kappa_T(r, s_1) = 2^y \left(\left\lceil \frac{r}{2^y} \right\rceil + \left\lceil \frac{s_1}{2^y} \right\rceil - 1 \right)$$

donde se supone, sin perdida de generalidad, que $x \leq y$. Entonces

$$\kappa_T(r, s_0) + \kappa_T(r, s_1) = 2^x \left(\left\lceil \frac{r}{2^x} \right\rceil + \left\lceil \frac{s_0}{2^x} \right\rceil - 1 + 2^{y-x} \left(\left\lceil \frac{r}{2^y} \right\rceil + \left\lceil \frac{s_1}{2^y} \right\rceil - 1 \right) \right).$$

Como $2^{y-x} \left\lceil \frac{s_1}{2^y} \right\rceil \geq \frac{s_1}{2^x}$ y $\lceil \xi_1 \rceil + \lceil \xi_2 \rceil \geq \lceil \xi_1 + \xi_2 \rceil$ para todo $\xi_1, \xi_2 \in \mathbb{R}$ se obtiene que $\kappa_T(r, s_0) + \kappa_T(r, s_1) \geq 2^x \left(\left\lceil \frac{r}{2^x} \right\rceil + \left\lceil \frac{s_0+s_1}{2^x} \right\rceil - 1 \right) \geq \kappa_{\widehat{H}}(r, s_0 + s_1)$. □

Si p es un entero mayor o igual que 2, se denota por $\oplus_p$ la suma Nim p-ádica la cual se define como sigue: sean k y l números naturales y $\sum_{i \geq 0} k_i p^i$, $\sum_{i \geq 0} l_i p^i$ las expansiones p-ádicas de k y l respectivamente, de ahí que $0 \leq k_i, l_i \leq p-1$ para todo i. La suma Nim p-ádica $k \oplus_p l$ es el entero cuya expansión p-ádica es $k \oplus_p l = \sum_{i \geq 0} (k_i \oplus_p l_i) p^i$, donde $k_i \oplus_p l_i$ denota el entero que está caracterizado por $0 \leq k_i \oplus_p l_i \leq p-1$ y $k_i \oplus_p l_i \equiv k_i + l_i (\text{mód} p)$.

Teorema 2.1. *Sea k un entero no negativo. En el grupo hamiltoniano $\widehat{H} = \mathcal{Q} \times (\mathbb{Z}/2\mathbb{Z})^k$ se cumple que $\mu_{\widehat{H}}(r, s) = \kappa_{\widehat{H}}(r, s)$ para todo par de enteros r, s tales que $1 \leq r, s \leq |\widehat{H}|$.*

Demostración. Dado que $\widehat{H}$ es soluble y que para cada $t \in \mathcal{H}(\widehat{H})$ existe un subgrupo normal de $\widehat{H}$ de orden t, el Lema 2.2 de [3] implica que $\mu_{\widehat{H}}(r, s) \leq \kappa_{\widehat{H}}(r, s)$. La prueba de la desigualdad $\mu_{\widehat{H}}(r, s) \geq \kappa_{\widehat{H}}(r, s)$ se hará por inducción sobre k. Para $k = 0$ tenemos $\widehat{H} = \mathcal{Q}$ y por el Lema 2.3 se cumple la afirmación. Supongamos

que la afirmación es cierta para el grupo hamiltoniano $\mathcal{T}$ de orden 2^{k+3} con $k \geq 0$, $\mu_{\mathcal{T}}(r,s) \geq \kappa_{\mathcal{T}}(r,s)$.

Sea $\widehat{H}$ un grupo hamiltoniano de orden 2^{k+4}, entonces existe un elemento c de orden 2 en el centro de $\widehat{H}$ tal que $\widehat{H} = \mathcal{T} \cup \mathcal{T}c$. Para enteros r y s tales que $1 \leq r, s \leq 2^{k+4}$ y dos subconjuntos A, B de $\widehat{H}$ que realizan a $\mu_{\widehat{H}}(r,s)$ se escogen subconjuntos $A_0, A_1, B_0, B_1 \subset \mathcal{T}$ de cardinales r_0, r_1, s_0, s_1, respectivamente, tales que $A = A_0 \cup A_1 c$ y $B = B_0 \cup B_1 c$. Así,

$$AB = (A_0B_0 \cup A_1B_1) \cup (A_0B_1 \cup A_1B_0)c$$

y por tanto

$$\mu_{\widehat{H}}(r,s) = |AB| = |A_0B_0 \cup A_1B_1| + |A_0B_1 \cup A_1B_0|\,. \tag{2}$$

Se consideran los siguientes casos:

1. Si $A_1 = B_1 = \varnothing$, entonces

   $$\mu_{\mathcal{T}}(r,s) \leq |A_0B_0| = |AB| = \mu_{\widehat{H}}(r,s) \leq \mu_{\mathcal{T}}(r,s).$$

   Luego, aplicando la hipótesis inductiva, $\mu_{\mathcal{T}}(r,s) \geq \kappa_{\mathcal{T}}(r,s) \geq \kappa_{\widehat{H}}(r,s)$, y por lo tanto

   $$\mu_{\widehat{H}}(r,s) \geq \kappa_{\widehat{H}}(r,s).$$

2. Los casos en que $A_1 = B_0 = \varnothing$, $A_0 = B_1 = \varnothing$ y $A_0 = B_0 = \varnothing$ se resuelven de manera similar al caso anterior.
3. Si $A_0 = \varnothing$ y $A_1, B_0, B_1 \neq \varnothing$, entonces

   $$\mu_{\widehat{H}}(r,s) = |A_1B_1| + |A_1B_0| \geq \mu_{\mathcal{T}}(r_1,s_1) + \mu_{\mathcal{T}}(r_1,s_0).$$

   De la hipótesis inductiva y el Lema 2.4 se deduce que

   $$\mu_{\widehat{H}}(r,s) \geq \kappa_{\mathcal{T}}(r,s_1) + \kappa_{\mathcal{T}}(r,s_0) \geq \kappa_{\widehat{H}}(r,s_0+s_1) = \kappa_{\widehat{H}}(r,s).$$

4. En los casos en que uno solo de los subconjuntos A_1, B_0 o B_1 es vacío, se procede de manera similar al caso 3.
5. Finalmente se supone que los conjuntos A_0, A_1, B_0, B_1 son no vacíos. De la igualdad (2) se tiene que

   $$\mu_{\widehat{H}}(r,s) \geq \max\{|A_0B_0|, |A_1B_1|\} + \max\{|A_0B_1|, |A_1B_0|\}\,,$$

   y por lo tanto

   $$\mu_{\widehat{H}}(r,s) \geq \max\{\mu_{\mathcal{T}}(r_0,s_0), \mu_{\mathcal{T}}(r_1,s_1)\} + \max\{\mu_{\mathcal{T}}(r_0,s_1), \mu_{\mathcal{T}}(r_1,s_0)\}\,.$$

   De la hipótesis inductiva se sigue que

   $$\mu_{\widehat{H}}(r,s) \geq \max\{\kappa_{\mathcal{T}}(r_0,s_0), \kappa_{\mathcal{T}}(r_1,s_1)\} + \max\{\kappa_{\mathcal{T}}(r_0,s_1), \kappa_{\mathcal{T}}(r_1,s_0)\}\,. \tag{3}$$

   Notemos que el conjunto $\mathbb{N}_0$ de los enteros no negativos tiene estructura de espacio vectorial sobre el campo finito $\mathbb{F}_2$, donde la suma de vectores es la suma Nim p-ádica. Sea $\mathcal{V}$ el subespacio de $\mathbb{N}_0$ generado por el conjunto $\{1, 2, 2^2, \ldots, 2^{k+2}\}$. Sea I_t el segmento inicial de longitud t de $\mathcal{V}$. De la Proposición 3.1 de [1] se sigue que

   $$\mu_{\mathcal{V}}(u,v) = |I_u \oplus_2 I_v| \quad \text{siempre que} \quad 1 \leq u, v \leq |\mathcal{V}|. \tag{4}$$

Sea $M = \mathcal{V} \times (\mathbb{Z}/2\mathbb{Z})$. Dado que M es abeliano y $\mathcal{H}(M) = \mathcal{H}(\widehat{H})$ se tiene

$$\mu_M(r,s) = \kappa_M(r,s) = \kappa_{\widehat{H}}(r,s). \tag{5}$$

Ahora, si el grupo $\mathcal{V}$ es visto como un subgrupo de M y se toma $b = (0,1) \in M$ se sigue que $M = \mathcal{V} \cup (\mathcal{V} + b)$. Sean $I_{r_0}, I_{r_1}, I_{s_0}, I_{s_1}$ los segmentos iniciales de $\mathcal{V}$ de longitudes r_0, r_1, s_0, s_1, respectivamente, y consideremos los conjuntos

$$E = I_{r_0} \cup (I_{r_1} + b) \quad \text{y} \quad D = I_{s_0} \cup (I_{s_1} + b).$$

Entonces

$$|E| = |I_{r_0} \cup (I_{r_1} + b)| = |I_{r_0}| + |I_{r_1}| = r_0 + r_1 = r,$$

$$|D| = |I_{s_0} \cup (I_{s_1} + b)| = |I_{s_0}| + |I_{s_1}| = s_0 + s_1 = s$$

y

$$E + D = [(I_{r_0} \oplus_2 I_{s_0}) \cup (I_{r_1} \oplus_2 I_{s_1})] \cup \{[(I_{r_0} \oplus_2 I_{s_1}) \cup (I_{r_1} \oplus_2 I_{s_0})] + b\}.$$

Así,

$$\mu_M(r,s) \leq |(I_{r_0} \oplus_2 I_{s_0}) \cup (I_{r_1} \oplus_2 I_{s_1})| + |(I_{r_0} \oplus_2 I_{s_1}) \cup (I_{r_1} \oplus_2 I_{s_0})|$$

De la igualdad (4) se tiene que

$$\mu_M(r,s) \leq \left|I_{\mu_{\mathcal{V}}(r_0,s_0)} \cup I_{\mu_{\mathcal{V}}(r_1,s_1)}\right| + \left|I_{\mu_{\mathcal{V}}(r_0,s_1)} \cup I_{\mu_{\mathcal{V}}(r_1,s_0)}\right|.$$

Por otro lado

$$I_{\mu_{\mathcal{V}}(r_0,s_0)} \cup I_{\mu_{\mathcal{V}}(r_1,s_1)} = I_{\max\{\mu_{\mathcal{V}}(r_0,s_0),\mu_{\mathcal{V}}(r_1,s_1)\}}$$

$$I_{\mu_{\mathcal{V}}(r_0,s_1)} \cup I_{\mu_{\mathcal{V}}(r_1,s_0)} = I_{\max\{\mu_{\mathcal{V}}(r_0,s_1),\mu_{\mathcal{V}}(r_1,s_0)\}}$$

implican que

$$\mu_M(r,s) \leq \max\{\mu_{\mathcal{V}}(r_0,s_0), \mu_{\mathcal{V}}(r_1,s_1)\} + \max\{\mu_{\mathcal{V}}(r_0,s_1), \mu_{\mathcal{V}}(r_1,s_0)\}.$$

Como $\mathcal{V}$ es abeliano, tenemos

$$\mu_M(r,s) \leq \max\{\kappa_{\mathcal{V}}(r_0,s_0), \kappa_{\mathcal{V}}(r_1,s_1)\} + \max\{\kappa_{\mathcal{V}}(r_0,s_1), \kappa_{\mathcal{V}}(r_1,s_0)\}.$$

Además $\mathcal{H}(T) = \mathcal{H}(\mathcal{V})$, luego

$$\mu_M(r,s) \leq \max\{\kappa_{\mathcal{T}}(r_0,s_0), \kappa_{\mathcal{T}}(r_1,s_1)\} + \max\{\kappa_{\mathcal{T}}(r_0,s_1), \kappa_{\mathcal{T}}(r_1,s_0)\}.$$

La desigualdad (3), la igualdad (5) y la desigualdad anterior implican que

$$\mu_{\widehat{H}}(r,s) \geq \kappa_{\widehat{H}}(r,s),$$

como se quería probar.

□

Teorema 2.2. *Sea k un entero no negativo. En el grupo $H = \mathcal{Q} \times (\mathbb{Z}/2\mathbb{Z})^k \times \mathcal{C}$, con $\mathcal{C} = \langle g \rangle$ un grupo cíclico de orden impar, se tiene que $\mu_H(r,s) = \kappa_H(r,s)$ para todo par de enteros positivos r, s tales que $1 \leq r, s \leq |H|$.*

Demostración. De los Lemas 1.2, 2.1 y 2.2 se deduce que $\mu_H(r,s) \leq \kappa_H(r,s)$. El elemento $b = (1,0,g)$ de H tiene orden n y pertenece al centro de H, por lo tanto

$$H = \widehat{H} \cup \widehat{H}b \cup \cdots \cup \widehat{H}b^{n-1},$$

donde $\widehat{H} = \mathcal{Q} \times (\mathbb{Z}/2\mathbb{Z})^k$.

Si A, B son subconjuntos de H que realizan $\mu_H(r,s)$, existen subconjuntos $A_{r_0}, \ldots, A_{r_{n-1}}$,
$B_{s_0}, \ldots, B_{s_{n-1}}$ de $\widehat{H}$ de cardinales $r_0, \ldots, r_{n-1}, s_0, \ldots, s_{n-1}$ respectivamente, tales que $\sum r_i = r$, $\sum s_i = s$,

$$A = \bigcup_{i=0}^{n-1} A_{r_i} b^i \qquad \text{y} \qquad B = \bigcup_{i=0}^{n-1} B_{s_i} b^i.$$

Si notamos $F_l = \{\ (i,j)\ :\ 0 \leq i,j \leq n-1,\ i+j \equiv l (\text{mód} n)\ \}$, tenemos que

$$AB = \left(\bigcup_{i=0}^{n-1} A_{r_i} b^i\right)\left(\bigcup_{j=0}^{n-1} B_{s_j} b^j\right) = \bigcup_{l=0}^{n-1}\left[\left(\bigcup_{(i,j)\in F_l} A_{r_i} B_{s_j}\right) b^l\right]$$

y por lo tanto

$$\begin{aligned}
\mu_H(r,s) &= |AB| = \sum_{l=0}^{n-1}\left|\bigcup_{(i,j)\in F_l} A_{r_i} B_{s_j}\right| \\
\mu_H(r,s) &\geq \sum_{l=0}^{n-1}(\text{máx}\{\ |A_{r_i} B_{r_j}|\ :\ (i,j)\in F_l\}) \\
&\geq \sum_{l=0}^{n-1}(\text{máx}\{\ \mu_{\widehat{H}}(r_i,s_j)\ :\ (i,j)\in F_l\}).
\end{aligned}$$

Del Teorema 2.1, se sigue que

$$\mu_H(r,s) \geq \sum_{l=0}^{n-1}(\text{máx}\{\ \kappa_{\widehat{H}}(r_i,s_j)\ |\ (i,j)\in F_l\}). \tag{6}$$

Sea $\mathcal{V}$ el subespacio de $\mathbb{N}_0$ generado por el conjunto $\{1, 2, 2^2, \ldots, 2^{k+2}\}$. Sea I_t el segmento inicial de longitud t de $\mathcal{V}$. La Proposición 3.1 de [1] implica que

$$\mu_{\mathcal{V}}(u,v) = |I_u \oplus_2 I_v| \quad \text{siempre que} \quad 1 \leq u,v \leq |\mathcal{V}|. \tag{7}$$

Sea $M = \mathcal{V} \times (\mathbb{Z}/n\mathbb{Z})$. Dado que M es abeliano y $\mathcal{H}(M) = \mathcal{H}(H)$ se tiene

$$\mu_M(r,s) = \kappa_M(r,s) = \kappa_H(r,s). \tag{8}$$

Si consideramos a $\mathcal{V}$ como un subgrupo de M, y tomamos $b = (0,1)$ en M, se sigue que $M = \bigcup_{k=0}^{n-1}(\mathcal{V} + kb)$. Sean $I_{r_0}, \ldots, I_{r_{n-1}}, I_{s_0}, \ldots, I_{s_{n-1}}$ los segmentos

iniciales de $\mathcal{V}$ de longitudes $r_0, \ldots, r_{n-1}, s_0, \ldots, s_{n-1}$ respectivamente. Sean E y D los conjuntos

$$E = \bigcup_{k=0}^{n-1} (I_{r_k} + kb) \quad \text{y} \quad D = \bigcup_{k=0}^{n-1} (I_{s_k} + kb).$$

Entonces

$$|E| = \sum_{k=0}^{n-1} r_k = r \quad \text{y} \quad |D| = \sum_{k=0}^{n-1} s_k = s$$

Además, si $F_l = \{\ (i,j)\ :\ 0 \leq i,j \leq n-1,\ i+j \equiv l(\text{mód}n)\}$,

$$E + D = \bigcup_{l=0}^{n-1} \left[\left(\bigcup_{(i,j)\in F_l} (I_{r_i} \oplus_2 I_{s_j}) \right) + lb \right].$$

Así que

$$\mu_M(r,s) \leq \sum_{l=0}^{n-1} \left| \left(\bigcup_{(i,j)\in F_l} I_{\mu_{\mathcal{V}}(r_i,s_j)} \right) \right|$$

Por otro lado, como

$$I_{\mu_{\mathcal{V}}(r_i,s_j)} \cup I_{\mu_{\mathcal{V}}(r_k,s_t)} = I_{\text{máx}\{\mu_{\mathcal{V}}(r_i,s_j),\mu_{\mathcal{V}}(r_k,s_t)\}}$$

se obtiene la desigualdad

$$\mu_M(r,s) \leq \sum_{l=0}^{n-1} \text{máx}\{\ \mu_{\mathcal{V}}(r_i,s_j)\ :\ (i,j) \in F_l\ \}.$$

Como $\mathcal{V}$ es abeliano, se tiene

$$\mu_M(r,s) \leq \sum_{l=0}^{n-1} \text{máx}\{\ \kappa_{\mathcal{V}}(r_i,s_j)\ :\ (i,j) \in F_l\ \}.$$

Además, como $\mathcal{H}(\widehat{H}) = \mathcal{H}(\mathcal{V})$, se sigue

$$\mu_M(r,s) \leq \sum_{l=0}^{n-1} \text{máx}\{\ \kappa_{\widehat{H}}(r_i,s_j)\ :\ (i,j) \in F_l\ \}.$$

La desigualdad (6), la igualdad (8) y la desigualdad anterior implican

$$\mu_H(r,s) \geq \kappa_H(r,s).$$

□

Agradecimientos

Los autores expresan su agradecimiento a la Universidad de Nariño, por el apoyo recibido durante la elaboración de este trabajo. Los autores son miembros de los grupos de investigación: Álgebra, Teoría de Números y Aplicaciones, ERM (ALTENUA) y Grupo de Investigación en Matemáticas y Educación Matemática (GESCAS). J.H. Castillo fue parcialmente financiado por CAPES y CNPq proc. 141857/2011-0 de Brasil.

Referencias

[1] S. Eliahou and M. Kervaire, Sumsets in vector spaces over finite fields, J. Number Theory **71** (1998), no. 1, 12–39. MR1631038 (99d:11020) 5, 7

[2] S. Eliahou and M. Kervaire, Minimal sumsets in infinite abelian groups, J. Algebra **287** (2005), no. 2, 449–457. MR2134154 (2006c:11018) 1

[3] S. Eliahou and M. Kervaire, Sumsets in dihedral groups, European J. Combin. **27** (2006), no. 4, 617–628. MR2215221 (2007a:11027) 2, 4

[4] S. Eliahou and M. Kervaire, The small sumsets property for solvable finite groups, European J. Combin. **27** (2006), no. 7, 1102–1110. MR2259941 (2008f:11116)

[5] S. Eliahou and M. Kervaire, Some results on minimal sumset sizes in finite non-abelian groups, J. Number Theory **124** (2007), no. 1, 234–247. MR2321003 (2008d:11022) 1, 2

[6] S. Eliahou and M. Kervaire, Bounds on the minimal sumsets size funtion in groups, J. Number Theory **4** (2007), 503–511. 2

[7] S. Eliahou and M. Kervaire, Minimal sumsets in finite solvable groups, Discrete Mathematics. **310** (2010), 471–479. 2

[8] W. Feit and J. G. Thompson, Solvability of groups of odd order. Pacific J. Math. **13** (1963), 775–1029. MR0166261. 3

[9] M. Hall Jr., The theory of groups. The Macmillan Co., New York, N.Y. (1959) xiii+434 pp. MR0103215. 3

[10] J. H. B. Kemperman, On complexes in a semigroup, Nederl. Akad. Wetensch. Proc. Ser. A. **59** = Indag. Math. **18** (1956), 247–254. MR0079005 (18,14a) 2

[11] D. J. S. Robinson, A course in the theory of groups. Graduate Texts in Mathematics, 80. Springer-Verlag, New York-Berlin, 1982. xvii+481 pp. ISBN: 0-387-90600-2 MR0648604 (84k:20001) 2

Wilson Fernando Mutis, Fernando Andrés Benavides y John Hermes Castillo
Facultad de Ciencias Exactas y Naturales
Departamento de Matemáticas y Estadística
Universidad de Nariño
San Juan de Pasto, Colombia
wfmutis@gmail.com, fandresbenavides@gmail.com y jhcastillo@gmail.com

Recibido: 7 de octubre de 2009
Revisado: 7 de diciembre de 2011
Aceptado: 2 de abril de 2012